コマンドライン インターフェイス

コマンド ライン インターフェイスの概要

AsyncOS コマンドライン インターフェイス（CLI）を使用して、Web Security Appliance を設定したりモニタすることができます。コマンドライン インターフェイスには、それらのサービスがイネーブルに設定されている IP インターフェイスで SSH を使用してアクセスするか、シリアル ポートで端末エミュレーション ソフトウェアを使用してアクセスできます。デフォルトでは、SSH は管理ポートに設定されます。

コマンドは、引数の有無を問わず、コマンド名を入力すると起動されます。引数を指定せずにコマンドを入力した場合は、必要な情報の入力を求めるプロンプトが表示されます。

コマンドライン インターフェイスへのアクセス

以下のいずれかの方法で接続できます。

- **イーサネット。**Web Security Appliance の IP アドレスを使用して SSH セッションを開始します。工場出荷時のデフォルト IP アドレスは 192.168.42.42 です。SSH は、ポート 22 を使用するように設定されています。
- **シリアル接続**シリアル ケーブルが接続されているパーソナル コンピュータの通信ポートを使用して、ターミナル セッションを開始します。

初回アクセス

admin アカウントを使用して初めて CLI にアクセスした後は、さまざまな許可レベルにより他のユーザを追加できます。以下のデフォルトの **admin** ユーザ名とパスフレーズを入力してアプライアンスにログインします。

- ユーザ名：**admin**
- パスフレーズ：**ironport**

デフォルトのパスフレーズで初めてログインすると、システム セットアップ ウィザードのプロンプトにより **admin** アカウントのパスフレーズを変更するよう求められます。

admin アカウントのパスフレーズは、passwd コマンドを使用していつでもリセットできます。

以降のアクセス

有効なユーザ名とパスフレーズを使用して、いつでもアプライアンス接続してログインできます。現在のユーザ名での最近のアプライアンスへのアクセス試行（成功、失敗を含む）の一覧が、ログイン時に自動的に表示されることに注意してください。

追加のユーザの設定については、userconfig コマンド、またはユーザ アカウントの管理（22-6 ページ）を参照してください。

コマンド プロンプトの使用

最上位のコマンド プロンプトは、完全修飾ホスト名に続いて大なり（>）記号とスペース 1 つで構成されます。次に例を示します。

```
example.com>
```

コマンドを実行すると、CLI によりユーザの入力が要求されます。CLI が入力を待機しているときは、プロンプトとして、角カッコ（[]）で囲まれたデフォルト値の後ろに大なり記号（>）が表示されます。デフォル値がない場合、カッコ内は空です。

次に例を示します。

```
example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

デフォルト設定がある場合は、コマンド プロンプトのカッコ内にその設定が表示されます。次に例を示します。

```
example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

デフォルト設定が表示されたときに Return キーを押すと、デフォルト値を受け入れたことになります。

コマンドの構文

インタラクティブ モードで動作している場合、CLI コマンド構文は単一のコマンドから構成されます。空白スペースを含まず、引数やパラメータもありません。次に例を示します。

```
example.com> logconfig
```

選択リスト

入力できる複数の選択肢がある場合、コマンドによっては番号付きリストを使用します。プロンプトで選択する番号を入力します。

次に例を示します。

```
Log level:
1. クリティカル(Critical)
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

Yes/No クエリー

yes または no のオプションがある場合、質問はデフォルト値（カッコ内表示）を付けて表示されます。**Y**、**N**、**Yes**、または **No** で返答できます。大文字と小文字の区別はありません。

次に例を示します。

```
Do you want to enable the proxy? [Y]> Y
```

サブコマンド

一部のコマンドでは、NEW、EDIT、DELETE などのサブコマンド命令を使用できます。EDIT および DELETE 機能では、設定済みの値のリストが表示されます。

次に例を示します。

```
example.com> interfaceconfig

Currently configured interfaces:

1. Management (172.xxx.xx.xx/xx: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.
```

```
- DELETE - Remove an interface.

[]>
```

サブコマンド内からメイン コマンドに戻るには、空のプロンプトで Enter または Return を入力します。

サブコマンドのエスケープ

サブコマンド内でいつでも Ctrl+C キーボード ショートカットを使用して、ただちに最上位の CLI に戻ることができます。

コマンド履歴

CLI は、セッション中に入力されたすべてのコマンドの履歴を保持します。最近使用したコマンドの実行リストをスクロールするには、キーボードの上下矢印キーを使用するか、Ctrl+P キーと Ctrl+N キーを組み合わせて使用します。

コマンドのオートコンプリート

AsyncOS CLI は、コマンド補完機能をサポートしています。コマンドの先頭の数文字を入力して Tab キーを押すと、CLI によって残りの文字列が補完されます。入力した文字が複数のコマンドに該当する場合、CLI はそのセットをさらに「絞り込み」ます。次に例を示します。

```
example.com> set （Tab キーを押す）
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth （もう一度 Tab キーを押すと sethostname での入力が完了）
```

CLI を使用した設定変更の確定

- 設定の変更の多くは、確定するまで有効になりません。
- commit コマンドを使用すると、他の操作を通常どおりに実行しながら設定を変更できます。
- 変更を正常に確定するには、最上位のコマンド プロンプトになっている必要があります。コマンド ライン階層の 1 つ上のレベルに移動するには、空のプロンプトで Return キーを押します。
- 確定されていない設定の変更は記録されますが、commit コマンドを実行するまで有効になりません。ただし、一部のコマンドは commit コマンドを実行しなくても有効になります。CLI セッションの終了、システムのシャットダウン、再起動、障害、または clear コマンドの発行により、確定されていない変更はクリアされます。
- ユーザが確認とタイムスタンプを受け取るまで、変更は実際に確定されません。

汎用 CLI コマンド

ここでは、変更の確定やクリアなど、一般的な CLI セッションで使用される基本的なコマンドについて説明します。

CLI の例:設定変更の確定

commit コマンドの後のコメントの入力は任意です。

```
example.com> commit


Please enter some comments describing your changes:

[]> Changed "psinet" IP Interface to a different IP address

Changes committed: Wed Jan 01 12:00:01 2007
```

CLI の例:設定変更のクリア

clear コマンドは、commit または clear コマンドが最後に実行された以降にアプライアンスの設定に対して行われた変更をすべてクリアします。

```
example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y

Changes cleared: Wed Jan 01 12:00:01 2007

example.com>
```

CLI の例:コマンドライン インターフェイス セッションの終了

exit コマンドを実行すると、CLI アプリケーションからログアウトされます。確定されていない設定変更はクリアされます。

```
example.com> exit

Configuration changes entered but not committed.Exiting will lose changes.

Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit?  [N]> y
```

CLI の例: コマンドライン インターフェイスでのヘルプの検索

help コマンドを実行すると、使用可能なすべての CLI コマンドが表示され、各コマンドの簡単な説明を参照できます。help コマンドは、コマンド プロンプトで help と入力するか、疑問符(?)を 1 つ入力して実行できます。

```
example.com> help
```

さらに、**help** *commandname* を入力して、特定のコマンドのヘルプにアクセスできます。

関連項目

- Web セキュリティ アプライアンスの CLI コマンド(B-6 ページ)

Web セキュリティ アプライアンスの CLI コマンド

Web セキュリティ アプライアンスの CLI は、システムへのアクセスおよびシステムのアップグレードと管理を実行する、一連のプロキシ コマンドと UNIX コマンドをサポートしています。

(注)　すべての CLI コマンドをすべての動作モード(標準および クラウド Web セキュリティ コネクタ)で適用/使用できるわけではありません。

コマンド(Command)	説明
adminaccessconfig	Web Security Appliance の設定で、アプライアンスにログインする管理者に対して厳しいアクセス要件を設け、非アクティブ タイムアウトの値を指定できます。詳細については、アプライアンスへのアクセスに対するセキュリティ設定の追加(22-12 ページ)とユーザ ネットワーク アクセス(22-14 ページ)を参照してください。

advancedproxyconfig	Web プロキシの詳細設定を設定します。サブコマンドは以下のとおりです。 **Authentication**：認証設定オプション。 • When would you like to forward authorization request headers to a parent proxy • Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog • Would you like to log the username that appears in the request URI • Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed) • Would you like to use advanced Active Directory connectivity checks • Would you like to allow case insensitive username matching in policies • Would you like to allow wild card matching with the character * for LDAP group names • Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8] • Would you like to enable referrals for LDAP • Would you like to enable secure authentication • Enter the hostname to redirect clients for authentication • Enter the surrogate timeout for user credentials • Enter the surrogate timeout for machine credentials • Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability • Enter re-auth on request denied option [disabled / embedlinkinblockpage] • Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication • Configure username and IP address masking in logs and reports

advancedproxyconfig (cont.)	**CACHING**：プロキシ キャッシュ モード。以下のうち 1 つを選択します。 • Safe Mode • Optimized Mode • Aggressive Mode • Customized Mode Web プロキシのキャッシュ モードの選択（4-7 ページ）も参照してください。 **DNS**：DNS 設定オプション。 • Enter the URL format for the HTTP 307 redirection on DNS lookup failure • Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure • Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive • Find web server by: 0 = Always use DNS answers in order 1 = Use client-supplied address then DNS 2 = Limited DNS usage 3 = Very limited DNS usage オプション 1 および 2 では、[Web レピュテーション（Web Reputation）] がイネーブルに設定されている場合、DNS が使用されます。オプション 2 および 3 では、DNS は、アップストリーム プロキシがない場合、または設定されたアップストリーム プロキシが失敗するイベントで、明示的なプロキシ要求に使用されます。すべてのオプションで、[宛先 IP アドレス（Destination IP Addresses）] がポリシー メンバーシップで使用されている場合、DNS が使用されます。 **EUN**：エンドユーザ通知パラメータ。 • Choose: 1. Refresh EUN pages 2. Use Custom EUN pages 3. Use Standard EUN pages • Would you like to turn on presentation of the User Acknowledgement page? Web プロキシ使用規約（4-11 ページ）とエンドユーザ通知の概要（17-1 ページ）も参照してください。 **NATIVEFTP**：ネイティブ FTP の設定。 • Would you like to enable FTP proxy • Enter the ports that FTP proxy listens on • Enter the range of port numbers for the proxy to listen on for passive FTP connections • Enter the range of port numbers for the proxy to listen on for active FTP connections • Enter the authentication format: 1. Check Point 2. No Proxy Authentication 3. Raptor • Would you like to enable caching • Would you like to enable server IP spoofing • Would you like to pass FTP server welcome message to the clients • Enter the max path size for the ftp server directory FTP プロキシ サービスの概要（4-15 ページ）も参照してください。

advancedproxyconfig（続き）	**FTPOVERHTTP**：FTP Over HTTP オプション。 • Enter the login name to be used for anonymous FTP access • Enter the password to be used for anonymous FTP access FTP プロキシ サービスの概要（4-15 ページ）も参照してください。 **HTTPS**：HTTPS 関連のオプション。 • HTTPS URI Logging Style - fulluri or stripquery • Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose • Would you like to decrypt HTTPS requests for End User Notification purpose • Action to be taken when HTTPS servers ask for client certificate during handshake: 1. Pass through the transaction 2. Reply with certificate unavailable • Do you want to enable server name indication (SNI) extension? • Do you want to enable automatic discovery and download of missing Intermediate Certificates? • Do you want to enable session resumption? HTTPS トラフィックを制御する復号化ポリシーの作成：概要（11-1 ページ）も参照してください。 **SCANNING**：スキャン オプション。 • Would you like the proxy to do malware scanning all content regardless of content type • Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds • Do you want to disable Webroot body scanning マルウェア対策 スキャンの概要（13-4 ページ）と発信トラフィックのスキャンの概要（12-1 ページ）も参照してください。 **PROXYCONN**：プロキシ接続ヘッダーを含むことができないユーザ エージェントのリストを管理します。リストのエントリは、Flex（Fast Lexical Analyzer）の正規表現として解釈されます。その文字列の一部がリスト内の正規表現のいずれかに一致するユーザ エージェントは、一致とされます。 • 実行する操作を選択します。 NEW - Add an entry to the list of user agents DELETE - Remove an entry from the list **CUSTOMHEADERS**：特定のドメインのカスタム要求ヘッダーを管理します。 • 実行する操作を選択します。 DELETE - Delete entries NEW - Add new entries EDIT - Edit entries Web 要求へのカスタム ヘッダーの追加（4-9 ページ）も参照してください。

advancedproxyconfig（続き）	**MISCELLANEOUS**：その他のプロキシ関連パラメータ。 • Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode) • Would you like proxy to perform dynamic adjustment of TCP receive window size • Would you like proxy to perform dynamic adjustment of TCP send window size • Enable caching of HTTPS responses • Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds) • Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds) • Mode of the proxy: 1. Explicit forward mode only 2. Transparent mode with L4 Switch or no device for redirection 3. Transparent mode with WCCP v2 Router for redirection • Spoofing of the client IP by the proxy: 1. Disable 2. Enable for all requests 3. Enable for transparent requests only • Do you want to pass HTTP X-Forwarded-For headers? • Do you want to enable server connection sharing? • Would you like to permit tunneling of non-HTTP requests on HTTP ports? • Would you like to block tunneling of non-SSL transactions on SSL Ports? • Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses? • Do you want proxy to throttle content served from cache? • Would you like the proxy to use client IP addresses from X-Forwarded-For headers • Do you want to forward TCP RST sent by server to client? • Do you want to enable URL lower case conversion for velocity regex? Web プロキシ データに対する P2 データ インターフェイスの使用（2-25 ページ）と Web プロキシの設定（4-3 ページ）も参照してください。 **SOCKS**：SOCKS プロキシのオプション。 • Would you like to enable SOCKS proxy • Proxy Negotiation Timeout • UDP Tunnel Timeout • SOCKS Control Ports • UDP Request Ports Web プロキシ データに対する P2 データ インターフェイスの使用（2-25 ページ）と SOCKS プロキシ サービス（4-17 ページ）も参照してください。

advancedproxyconfig（続き）	**CONTENT-ENCODING**：コンテンツエンコーディング タイプを許可およびブロックします。 現在許可されているコンテンツエンコーディング タイプ：compress、deflate、gzip 現在ブロックされているコンテンツエンコーディング タイプ：該当なし 特定のコンテンツエンコーディング タイプの設定を変更するには、次のオプションを選択します。 1. compress 2. deflate 3. gzip [1]> The encoding type "compress" is currently allowed Do you want to block it? [N]>
alertconfig	アラートの受信者を指定し、システム アラートを送信するためのパラメータを設定します。
authcache	認証キャッシュから 1 つまたはすべてのエントリ（ユーザ）を削除できるようにします。また、その時点で認証キャッシュに含まれているすべてのユーザのリストを表示できます。
bwcontrol	デフォルトのプロキシ ログ ファイルの帯域幅制御デバッグ メッセージを有効にします。
certconfig	**SETUP**：セキュリティ証明書とキーを設定します。
クリア	前回の確定以降の保留されている設定変更をクリアします。
commit	システム設定に対する保留中の変更を確定します。
createcomputerobject	指定された場所にコンピュータ オブジェクトを作成します。
curl	cURL 要求を、Web サーバに直接またはプロキシ経由で送信します。要求および返される応答の HTTP ヘッダーから、Web ページをロードできなかった理由を判別できます。 **（注）** このコマンドは、TAC の監督のもとで管理者またはオペレータだけが使用できます。 サブコマンドは次のとおりです: **DIRECT**：直接 URL アクセス **APPLIANCE**：アプライアンス経由での URL アクセス
datasecurityconfig	要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は Cisco データ セキュリティ フィルタによってスキャンされません。
date	現在の日付を表示します。例: `Thu Jan 10 23:13:40 2013 GMT`

diagnostic	プロキシおよびレポート関連のサブコマンド: **NET**:ネットワーク診断ユーティリティ このコマンドは廃止されました。アプライアンスでネットワーク トラフィックをキャプチャするには、packetcapture を使用します。 **PROXY**:プロキシ デバッグ ユーティリティ 実行する操作を選択します。 – SNAP:プロキシのスナップショットを取得します。 – OFFLINE:プロキシをオフラインにします(WCCP 経由)。 – RESUME:プロキシのトラフィックを再開します(WCCP 経由)。 – CACHE:プロキシのキャッシュをクリアします。 **REPORTING**:レポート ユーティリティ レポート システムは現在有効になっています。 実行する操作を選択します。 – DELETEDB:レポート データベースを再度初期化します。 – DISABLE:レポート システムを無効にします。 – DBSTATS:データベースおよびエクスポート ファイルをリストします (export_files および always_onbox フォルダの下の未処理のファイルおよびフォルダのリストを表示します)。 – DELETEEXPORTDB:エクスポート ファイルを削除します (export_files および always_onbox フォルダの下の未処理のファイルおよびフォルダをすべて削除します)。 – DELETEJOURNAL:ジャーナル ファイルを削除します (すべての aclog_journal_files を削除します)。
dnsconfig	DNS サーバのパラメータを設定します。
dnsflush	アプライアンスの DNS エントリをフラッシュします。
etherconfig	イーサネット ポート接続を設定します。
externaldlpconfig	要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は外部 DLP サーバでスキャンされません。
featurekey	有効なキーを送信して、ライセンスされた機能をアクティブ化します。
featurekeyconfig	自動的に機能キーをチェックして更新します。
grep	名前付き入力ファイルを検索して、特定のパターンに一致するものを含む行を見つけます。
ヘルプ	コマンドのリストを返します。
iccm_message	この Web Security Appliance がセキュリティ管理アプライアンス(M-Series)によって管理される時期を示すメッセージを、Web インターフェイスと CLI からクリアします。
ifconfig または interfaceconfig	M1、P1、P2 などのネットワーク インターフェイスを設定して管理します。現在設定されているインターフェイスを表示し、インターフェイスを作成、編集、削除する操作メニューを提供します。

iseconfig	現在の ISE 設定パラメータを表示します。実行する ISE 設定操作を指定できます。 • setup：ISE の設定項目を設定します（有効化/無効化、ISE サーバ名または IPv4 アドレス、プロキシ キャッシュのタイムアウト、統計情報のバックアップ間隔）。
isedata	ISE データ関連の操作を指定します。 statistics：ISE サーバのステータスと ISE 統計情報を表示します。 cache：ISE キャッシュを表示するか、IP アドレスを確認します。 show：ISE ID キャッシュを表示します。 checkip：IP アドレスのローカル ISE キャッシュをクエリします。 sgts：ISE セキュア グループ タグ（SGT）テーブルを表示します。
last	tty やホストなどのユーザ固有のユーザ情報を新しい順に並べて一覧表示したり、指定した日時にログインしたユーザのリストを表示します。
loadconfig	システム コンフィギュレーション ファイルをロードします。
logconfig	ログ ファイルへのアクセスを設定します。
mailconfig	指定されたアドレスに現在のコンフィギュレーション ファイルをメールで送信します。
maxhttpheadersize	プロキシ要求の最大 HTTP ヘッダー サイズを設定します。値をバイト単位で入力するか、キロバイトを表す場合は数値に K を付記します。 多数の認証グループに属するユーザの場合はポリシー トレースが失敗する可能性があります。また、HTTP 応答ヘッダーのサイズが現在の「最大ヘッダー サイズ」よりも大きい場合、失敗することがあります。この値を大きくすると、このような障害を軽減できます。最小値は 32 KB、デフォルト値は 32 KB、最大値は 1024 KB です。
musconfig	このコマンドを使用して Secure Mobility を有効化し、リモート ユーザの識別方法を設定します（IP アドレスによって識別するか、1 つ以上の Cisco 適応型セキュリティ アプライアンスと統合することで識別）。 （注）　このコマンドを使って変更すると、Web プロキシが再起動されます。
musstatus	Web Security Appliance を適応型セキュリティ アプライアンスと統合したときに、このコマンドを使用して Secure Mobility に関連する情報を表示します。 このコマンドにより、以下の情報が表示されます。 • Web Security Appliance と個々の適応型セキュリティ アプライアンスとの接続の状態。 • Web Security Appliance と個々の適応型セキュリティ アプライアンスとの接続時間（分単位）。 • 個々の適応型セキュリティ アプライアンスからのリモート クライアントの数。 • サービス対象のリモート クライアントの数。これは、Web Security Appliance を介してトラフィックの受け渡しを行ったリモート クライアントの数です。 • リモート クライアントの合計数。

networktuning	WSA は、複数のバッファおよび最適化アルゴリズムを使用して数百もの TCP 接続を同時に処理し、一般的な Web トラフィック（つまり、一時的な HTTP 接続）に対して高いパフォーマンスを実現します。 大容量ファイル（100 MB 以上）が頻繁にダウンロードされるような特定の状況では、バッファが大きいほど接続ごとのパフォーマンスが向上する可能性があります。ただし、全体的なメモリ使用量が増加するため、システムで使用可能なメモリに応じてバッファを増やす必要があります。 送信および受信スペース変数は、指定の TCP ソケットを介した通信用にデータを保存するために使用されるバッファを表します。自動送信および受信変数は、ウィンドウ サイズを動的に制御するための FreeBSD 自動調整アルゴリズムを有効または無効にするために使用されます。これら 2 つのパラメータは、FreeBSD カーネルに直接適用されます。 **SEND_AUTO** と **RECV_AUTO** が有効な場合、システムの負荷と使用可能なリソースに基づいてウィンドウ サイズが動的に調整されます。負荷が小さい WSA では、トランザクションあたりの遅延を削減するためウィンドウ サイズが大きく維持されます。動的に調整されるウィンドウ サイズの最大値は、設定されている mbuf クラスタの数に依存します。つまり、システムで使用可能な RAM の合計に応じて異なります。クライアント接続の合計数が増加する場合、または使用可能なネットワーク バッファ リソースが非常に少なくなる場合には、すべてのネットワーク バッファ リソースがプロキシ トラフィックにより使用されることを防いでシステムを保護するため、ウィンドウ サイズが削減されます。 このコマンドの使用に関する詳細については、アップロード/ダウンロード速度の問題（A-7 ページ）を参照してください。 networktuning サブコマンドは、次のとおりです。 **SENDSPACE**：TCP 送信スペースのバッファ サイズ。8192 ～ 262144 バイトの範囲で、デフォルトは 32768 バイトです。 **RECVSPACE**：TCP 受信スペースのバッファ サイズ。8192 ～ 262144 バイトの範囲で、デフォルトは 65536 バイトです。 **SEND_AUTO**：TCP 送信の自動調整を有効/無効にします。1 はオン、0 はオフ（デフォルトはオフ）。TCP 送信の自動調整を有効にする場合、必ず advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP send window size? の順に使用して、送信バッファの自動調整を無効にしてください。 **RECV_AUTO**：TCP 受信の自動調整を有効/無効にします。1 はオン、0 はオフ（デフォルトはオフ）。TCP 受信の自動調整を有効にする場合、必ず advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP receive window size? の順に使用して、受信バッファの自動調整を無効にしてください。 **MBUF_CLUSTER_COUNT**：使用可能な mbuf クラスタの数を変更します。許容範囲は 98304 ～ 147146（デフォルトは 98304）。この値は、インストールされたシステム メモリによって変わります。98304 * (X/Y) の計算を使用し、X はシステム上の RAM のギガバイトで、Y は 4 GB です。たとえば 4 GB RAM の場合、推奨値は 98304 * (4/4) = 98304 になります。RAM が増加する場合は、線形スケーリングが推奨されます。スケーリングされた値よりも小さい値は指定できますが、大きい値は指定できません。 **SENDBUF_MAX**：最大送信バッファ サイズを指定します。範囲は 131072 ～ 524288 バイト、デフォルトは 256 KB（262144 バイト）。

networktuning（続き）	**RECVBUF_MAX**：最大受信バッファ サイズを指定します。範囲は 131072 ～ 524288 バイト、デフォルトは 256 KB（262144 バイト）。 **CLEAN_FIB_1**：データルーティング テーブルからすべての M1/M2 エントリを削除します。基本的には、コントロールプレーン/データプレーンの分離を有効にします。つまり、「分離ルーティング」が有効になっている場合に M1 インターフェイス経由のデータ送信からデータプレーン プロセスを無効にします。データプレーン プロセスは、「データ ルーティング テーブルの使用」が有効になっているプロセス、または非管理トラフィックを厳密に伝達するプロセスです。コントロールプレーン プロセスでは、依然として M1 または P1 インターフェイスのいずれかを介してデータを送信できます。 これらのパラメータに何らかの変更を行った後は、必ず変更を確定してアプライアンスを再起動してください。 ⚠ **注意**　副次的な影響を理解している場合にのみ、このコマンドを使用してください。TAC ガイダンスを受けている場合にのみ使用することを推奨します。
nslookup	指定されたホストとドメインの情報を得るために、またはドメイン内のホストのリストを印刷するために、インターネット ドメイン ネーム サーバに照会します。
ntpconfig	NTP サーバの設定現在設定されているインターフェイスを表示し、インターフェイスを追加、削除、または設定する操作メニューを提供します。このインターフェイスの IP アドレスから NTP クエリーが発信されます。
packetcapture	アプライアンスが接続されているネットワーク上で送受信されている TCP/IP などのパケットを代行受信して表示します。
passwd	パスフレーズを設定します。
pathmtudiscovery	パス MTU ディスカバリをイネーブルまたはディセーブルにします。 パケット フラグメンテーションが必要な場合は、パス MTU ディスカバリをディセーブルにすることができます。
ping	指定されたホストまたはゲートウェイに ICMP エコー要求を送信します。
proxyconfig <enable | disable>	Web プロキシをイネーブルまたはディセーブルにします。
proxystat	Web プロキシの統計情報を表示します。
quit, q, exit	アクティブなプロセスまたはセッションを終了します。
reboot	ファイル システム キャッシュをディスクにフラッシュし、実行中のすべてのプロセスを停止して、システムを再起動します。
reportingconfig	レポーティング システムを設定します。
resetconfig	出荷時の初期状態に設定を復元します。
revert	Web オペレーティング システム用の AsyncOS を以前の認定済みビルドに復元します。これは非常に危険な操作で、すべての設定ログおよびデータベースを破棄します。このコマンドの使用については、以前のバージョンの AsyncOS for Web への復元（22-39 ページ）を参照してください。
rollovernow	ログ ファイルをロール オーバーします。

routeconfig	トラフィックの宛先 IP アドレスとゲートウェイを設定します。現在設定されているルートを表示し、エントリを作成、編集、削除、クリアする操作メニューを提供します。
saveconfig	現在の設定のコピーをファイルに保存します。必要に応じて、このファイルを使用してデフォルトを復元できます。
setgateway	マシンのデフォルト ゲートウェイを設定します。
sethostname	hostname パラメータを設定します。
setntlmsecuritymode	NTLM 認証レルムのセキュリティ設定を、「ads」または「domain」に変更します。 • domain：AsyncOS は Active Directory ドメインにドメイン セキュリティ信頼アカウントを結合します。AsyncOS では、Active Directory はこのモードでネストされた Active Directory グループだけを使用する必要があります。 • ads：AsyncOS は、Active Directory のネイティブ メンバーとしてドメインを結合します。 デフォルト設定は ads です。
settime	システム時刻を設定します。
settz	現在のタイム ゾーンとタイム ゾーンのバージョンを表示します。ローカル タイム ゾーンを設定する操作メニューを提供します。
showconfig	すべての設定値を表示します。 (注)　ユーザのパスフレーズは暗号化されます。
shutdown	接続を終了してシステムをシャット ダウンします。
smtprelay	内部的に生成された電子メールの SMTP リレー ホストを設定します。SMTP リレー ホストは、システムで生成された電子メールやアラートを受け取るために必要です。
snmpconfig	SNMP クエリーをリッスンし、SNMP 要求を受け入れるようにローカル ホストを設定します。
sshconfig	信頼できるサーバのホスト名とホスト キー オプションを設定します。 SSHD：SSH サーバの構成設定を編集します。 USERKEY：SSH ユーザ キーの設定を編集します。

sslconfig	アプライアンス管理 Web ユーザ インターフェイス、プロキシ サービス（HTTPS プロキシ、セキュア クライアントのクレデンシャル暗号化など）、セキュア LDAP サービス（認証、外部認証、セキュア モビリティなど）、アップデート サービスにおける、通信プロトコル TLS v1.x および SSL v3 の使用に関するコマンド。 VERSIONS：特定のサービスでイネーブルであるプロトコルを表示および変更します。 COMPRESS：TLS 圧縮をイネーブルまたはディセーブルにします。最高のセキュリティのためにディセーブルに設定することが推奨されます。 CIPHERS：選択したプロトコルで使用可能な追加/アップデート暗号スイートを追加します。 AsyncOS バージョン 9.0 以前のデフォルトの暗号は、DEFAULT:+kEDH です。AsyncOS バージョン 9.1 以降では、デフォルトの暗号は EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA になります。いずれの場合も、ECDHE 暗号の選択によって変わる可能性があります。 （注）　ただし、バージョンに関係なく、新しい AsyncOS バージョンにアップグレードする際にデフォルトの暗号は変わりません。たとえば、以前のバージョンから AsyncOS 9.1 にアップグレードする場合、デフォルトの暗号は DEFAULT:+kEDH です。つまり、アップグレード後に、現在の暗号スイートを自分で更新する必要があります。シスコでは、EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA への更新を推奨します。 FALLBACK：SSL/TLS のフォールバック オプションをイネーブルまたはディセーブルにします。イネーブルの場合、リモート サーバとの通信は、ハンドシェイクの失敗後、最も低く設定されているプロトコルにフォールバックします。 プロトコル バージョンがクライアントとサーバの間でネゴシエートされると、実装の問題が原因でハンドシェイクが失敗する可能性があります。このオプションがイネーブルの場合、プロキシは現在設定されている TLS/SSL プロトコルの最も低いバージョンを使用して接続を試みます。 （注）　AsyncOS 9.x の新規インストール時、フォールバックはデフォルトでディセーブルに設定されています。フォールバック オプションがある以前のバージョンからアップグレードする場合、現在の設定が保持されます。そうでない場合、つまりこのオプションがないバージョンからアップグレードする場合、フォールバックはデフォルトでイネーブルに設定されています。 ECDHE：LDAP での ECDHE 暗号の使用をイネーブルまたはディセーブルにします。 その後のリリースで追加の ECDH 暗号がサポートされていますが、追加の暗号とともに提供された特定の名前付き曲線が原因で、セキュア LDAP 認証と HTTPS トラフィック復号化の際中に、アプライアンスが接続をクローズする場合があります。追加の暗号の指定については、SSL の設定（22-25 ページ）を参照してください。 これらの問題がある場合は、このオプションを使用して、一方または両方の機能で ECDHE 暗号の使用をディセーブルにするか、またはイネーブルにします。

status	システム ステータスを表示します。
supportrequest	サポート要求の電子メールを Cisco カスタマー サポートに送信します。これには、マスター設定のコピーおよびシステム情報が含まれます。

tail	ログ ファイルの末尾を表示します。コマンドには、ログ ファイル名または番号をパラメータとして指定できます。
	`example.com> tail system_logs`
	`example.com> tail 9`

tcpservices	開かれている TCP/IP サービスに関する情報を表示します。
techsupport	Cisco カスタマー サポートがシステムにアクセスしてトラブルシューティングを支援できるように、一時的な接続を提供します。
telnet	TELNET プロトコルを使用して別のホストと通信します。通常、接続の確認に使用されます。
testauthconfig	特定の認証レルムで定義された認証サーバに対して、そのレルムの認証設定をテストします。 `testauthconfig [-d level] [realm name]` オプションを指定せずにコマンドを実行すると、設定されている認証レルムのリストが表示されるので、そのリストから選択できます。 デバッグ フラグ（`- d`）によってデバッグ情報のレベルが制御されます。指定できるレベルの範囲は 0～10 です。指定しない場合は、レベル 0 が使用されます。レベル 0 の場合は、コマンドによって成功または失敗が返されます。テスト設定が失敗すると、失敗の原因が一覧表示されます。 **（注）** レベル 0 を使用することを推奨します。トラブルシューティングのためにさらに詳細な情報が必要な場合にのみ、別のデバッグ レベルを使用してください。
traceroute	ゲートウェイを通過し、宛先ホストまでのパスをたどって、IP パケットをトレースします。
tuiconfig tuistatus	これらの 2 つのコマンドについては、CLI を使用した透過的ユーザ識別の詳細設定（5-10 ページ）で説明しています。
updateconfig	アップデートおよびアップグレードを設定します。
updatenow	すべてのコンポーネントを更新します。

アップグレード	AsyncOS ソフトウェアのアップグレードをインストールします。 downloadinstall：アップグレード パッケージをダウンロードし、即時にインストールします。 download：アップグレード パッケージをダウンロードし、後でインストールできるように保存します。 いずれかのコマンドを入力すると、この WSA に適用可能なアップグレード パッケージのリストが表示されます。使用するパッケージのエントリ番号を入力してそのパッケージを選択し、Enter キーを押します。ダウンロードがバックグラウンドで開始されます。ダウンロード中に、サブコマンド downloadstatus と canceldownload を使用できます。 最初に downloadinstall を入力した場合、ダウンロードが完了するとインストールが即時に開始されます。download を入力した場合は、ダウンロード完了時に 2 つのコマンド（install と delete）が使用可能になります。install と入力すると、以前にダウンロードしたパッケージのインストールが開始します。delete と入力すると、以前にダウンロードしたパッケージが WSA から削除されます。
userconfig	システム管理者を設定します。
version	一般的なシステム情報、インストールされているシステム ソフトウェアのバージョン、およびルールの定義を表示します。
wccpstat	all：すべての WCCP（Web Cache Communication Protocol）サービス グループの詳細を表示します。 servicegroup：特定の WCCP サービス グループの詳細を表示します。
webcache	プロキシ キャッシュの内容を確認または変更したり、アプライアンスにキャッシュされないドメインと URL を設定します。管理者は特定の URL をプロキシ キャッシュから削除したり、プロキシ キャッシュに保存しないドメインや URL を指定できます。
who	CLI および Web インターフェイス セッションの両方について、システムにログインしているユーザを表示します。 **（注）**　各ユーザは、最大 10 の同時セッションを持つことができます。
whoami	ユーザ情報を表示します。